Aufbewahrung und Archivierung

Einleitung zur Archivierung

In Fitness-Centren fallen täglich Daten an, die auch personenbezogene Angaben über Kunden und Mitarbeiter sowie Dienstleister enthalten. Die Aufbewahrung dieser Daten und Dokumente erfolgt gemäss dem Prinzip von gesetzlichen Vorgaben Verhältnismässigkeit. Art. 6 Abs. 4 DSG besagt, dass Personendaten nach Erreichung des Zwecks zu löschen sind oder anonymisiert werde müssen. Personenbezogene Daten dürfen daher nur so lange aufbewahrt werden, wie sie für die Erfüllung der Aufgaben geeignet und erforderlich sind. Bundesgesetze und evtl. kantonale Vorschriften legen ausserdem weitere konkrete Aufbewahrungsfristen fest.

Geschäftsdaten, die anonymisiert wurden oder keine personenbezogenen Daten enthalten, können grundsätzlich unbegrenzt aufbewahrt werden. Mindestens müssen sie jedoch für die Dauer aufbewahrt werden, die gesetzlich vorgesehen ist.

Gesetzliche Aufbewahrungsfristen

Die folgenden Tabellen geben einen Überblick über die gesetzlichen Anforderungen an die Art und Dauer der Aufbewahrung. Wenn keine gesetzlichen Regelungen zur Aufbewahrung bestehen, schreibt das Datenschutzgesetz vor, dass zumindest die Kriterien für die Aufbewahrung festgelegt werden müssen (Art. 12 DSG).

Während der gesamten Aufbewahrungsdauer muss sichergestellt sein, dass der Datenschutz und insbesondere die Datensicherheit gewährleistet bleiben. Ein letzter Abschnitt dieses Kapitels enthält eine Checkliste mit möglichen technischen und organisatorischen Massnahmen zur Aufrechterhaltung der Datensicherheit.

Nachfolgend eine nicht abschliessende mögliche Liste zur Archivierung.

Kunden		
Art der Unterlagen	Aufbewahrungsdauer und Art	Grundlage
Kundenverträge und Mitgliedschaftsunterlagen	10 Jahre nach Vertragsende; evtl. sogar 20 Jahre im Zusammenhang mit der nachfolgenden Pflicht zur Aufbewahrung Haftpflicht.	Obligationenrecht (OR)
Gesundheitsfragebögen und medizinische Unterlagen	Aufgrund von Verjährungsfristen im Haftungsrecht (vertragswidrige Körperverletzung) ist die Dokumentation bis 20 Jahre nach Abschluss der Trainings, Behandlungen aufzubewahren. Darüber hinaus darf sie nur mit der Zustimmung der betroffenen Person aufbewahrt bleiben.	Art. 60 Abs. 1bis und 2 Obligationenrecht (OR)/Art. 128a OR
Trainingspläne und -protokolle	20 Jahre nach Vertragsende	Keine spezifische gesetzliche Regelung, aber notwendig für die Leistungserbringung

Mitarbeiter		
Art der Unterlagen	Aufbewahrungsdauer und Art	Rechtliche Grundlage
Mitarbeiterverträge und Personaldossier	Mind. 5 Jahre ab Austritt der/des Mitarbeitenden, besser 10 Jahre wegen des Rechts auf Arbeitszeugnis, das erst nach 10 Jahren verjährt, sodass der Sachverhalt nachgewiesen werden kann.	Art. 330a OR i.V. Art. 128 OR/Art. 46 Arbeitsgesetz (ArG) und 73 Verordnung 1 zum Arbeitsgesetz (ArGV 1)
Lohnwesen	10 Jahre ab Austritt der/des Mitarbeitenden	Art. 128 Abs. 3 OR
Arbeitszeiterfassung	10 Jahre ab Austritt der/des Mitarbeitenden	Art. 46 Arbeitsgesetz (ArG) und 73 Verordnung 1 zum Arbeitsgesetz (ArGV 1)
Unternehmen		
Art der Unterlagen	Aufbewahrungsdauer und Art	Rechtliche Grundlage
Rechnungen	10 Jahre ab Beendigung des Geschäftsjahres	Art. 958 und 958f OR
Steuerunterlagen		
Spesen		
Sonstige Dokumentation		
Protokolle bei automatisierter Bearbeitung von besonders schützenswerten Personendaten (Profiling)	1 Jahr, sofern besonders schützenswerte Personendaten automatisiert bzw. digitalisiert bearbeitet und die eingesetzten Massnahmen keinen genügenden Datenschutz bieten, hat sie die Bearbeitung zu protokollieren. Die Protokolle sind während 1 Jahr revisionsgerecht aufzubewahren.	Art. 4 Verordnung über den Datenschutz (DSV)
Datenschutz-Folgenabschätzung (DSFA)	Mindestens 2 Jahre ab Beendigung der Datenbearbeitung.	Art. 14 DSV
Dokumentation Verletzung der Datensicherheit	Mindestens zwei Jahre ab dem Zeitpunkt der Meldung einer Verletzung der Datensicherheit.	Art. 15 DSV

Rechtliche Grundlagen Löschung

Die oben genannten Informationen beziehen sich auf den Umgang mit personenbezogenen Daten gemäss Artikel 6 Absatz 4 DSG. Gemäss diesem Artikel dürfen personenbezogene Daten nur für den bestimmten Zweck bearbeitet werden, für den sie erhoben wurden, und nur in dem Umfang, der für diesen Zweck geeignet und erforderlich ist.

Sobald die personenbezogenen Daten für den ursprünglichen Zweck nicht mehr erforderlich sind, müssen sie gelöscht, vernichtet oder anonymisiert werden. Dies bedeutet, dass die Daten nicht länger in einer Form gespeichert werden dürfen, die die Identifizierung der betroffenen Person ermöglicht.

Betroffene Personen haben das Recht, die Löschung ihrer personenbezogenen Daten zu verlangen, wenn es keine Rechtfertigungsgründe mehr für deren Bearbeitung gibt. Rechtfertigungsgründe können beispielsweise gesetzliche Aufbewahrungs- oder Verjährungsfristen sein oder die Aufbewahrung wegen einem Rechtsstreit oder zur Vertragserfüllung. Diese Fristen können je nach Situation unterschiedlich geregelt sein.

Das Vorgehen bei einem Gesuch auf Löschung:

1. Die identifizierende Person: Die Person, die das Löschungsgesuch stellt, muss eindeutig identifiziert werden, um sicherzustellen, dass die richtigen personenbezogenen Daten gelöscht werden.

2. Überprüfung von Aufbewahrungspflichten: Es muss geprüft werden, ob gesetzliche Aufbewahrungspflichten oder andere zwingende Gründe gegen eine Löschung der Daten sprechen. Wenn keine solchen Gründe vorliegen, müssen die personenbezogenen Daten gelöscht oder vernichtet werden.

3. Rückmeldung an die betroffene Person: Die betroffene Person muss über das Ergebnis des Löschungsgesuchs informiert werden. Wenn die Daten nicht gelöscht wurden, muss die Begründung dafür angegeben werden.

Technische Anforderungen an die Löschung

Definition der Löschung/Vernichtung

Mit dem Begriff der Vernichtung von Daten ist in der Regel die physische Vernichtung von Daten oder die unwiderrufliche Löschung von digitalen Daten gemeint. Während unter der physischen Vernichtung die Zerstörung eines Datenträgers (Papierdokumente, USB-Sticks, CDs etc.) verstanden wird, fällt unter den Begriff der Löschung die Unkenntlichmachung von gespeic herten Daten. Anders als bei der Vernichtung bleibt der Datenträger bei der Löschung erhalten. Ebenfalls kann die Verschlüsselung von Daten als löschen angesehen werden, wenn die zugehörigen Schlüssel, für die Entschlüsselung, unwiederbringlich entsorgt werden.

Back-ups sind in das Löschkonzept einzubeziehen

Ein Back-up ist zwingend zum Schutz vor Datenverlust zu installieren. Back-ups mit kurzen Sicherungszyklen (z. B. täglich, wöchentlich, monatlich) werden üblicherweise regelmässig überschrieben und können daher im Zusammenhang mit dem Löschen auch ignoriert werden, denn wenn die Livedaten gelöscht werden, verschwinden diese Daten demnach in den folgenden Back-ups ebenfalls.

In Back-ups mit langen Sicherungszyklen (z. B. jährlich) hingegen bleiben diese Daten weiterhin vorhanden. Im Falle einer Wiederherstellung würden diese Daten rekonstruiert, womit die Löschung der Daten rückgängig gemacht wird.

Um sicherzustellen, dass gelöschte Daten auch nach der Wiederherstellung eines Back-ups gelöscht bleiben, empfiehlt es sich, einen Prüfprozess einzurichten. Dabei kann beispielsweise eine Liste geführt werden, auf welcher mit pseudonymisierten Daten (z.B. Kundennummer und Löschdatum) festgehalten wird, welche Datensätze gelöscht wurden. Im Fall der Wiederherstellung, kann anhand dieser Liste geprüft werden, ob auch gelöschte Datensätze wiederhergestellt wurden und allfällig nach der Wiederherstellung gelöscht werden.

Eingeschränkte Zugriffsrechte auf Back-ups sind durch technische und organisatorische Massnahmen sicherzustellen.

E-Mails

Sofern E-Mails Kundendaten und insbesondere besonders schützenswerte enthalten, der Kunden beinhalten, sind sie in der Kundenakte abzulegen. Wenn die Akte gemäss den gesetzlich vorgegebenen Aufbewahrungsfristen gelöscht wird, ist sicherzustellen, dass die damit verbundenen E-Mails ebenso gelöscht werden.

Sicherheitsanforderungen an die Löschung

Die gewählten Löschmethode hat eine unwiederbringliche Löschung zu gewährleisten. Dies bedeutet, dass die Methode zu wählen ist, welche die Wiederherstellung der gelöschten Personendaten verunmöglicht. Nicht datenschutzkonform ist die einfache Entsorgung von Personendaten in Abfallsäcken/Müllcontainern oder das Verschieben einer Datei in den «digitalen Papierkorb».

Sicherheitsanforderung an die Löschung

Art der Vernichtung	Beschreibung	Bewertung
Physische Vernichtung	Mechanische Zerstörung eines Datenträgers (Schreddern, Einschmelzen etc.).	Datenschutzkonforme Löschung gewährleistet.
Magnetische Löschung	Spezielle Löschgeräte ermöglichen das Löschen von Informationen ganzer Festplatten durch Magnetisierung.	Unwiderruflichkeit der Löschung gegeben, Datenträger werden funktionsunfähig.
Wipen/technisches Überschreiben	Mehrfaches Überschreiben von Dateien oder ganzen Speichermedien mit zufälligen Zeichenfolgen.	Unwiderruflichkeit der Vernichtung gegeben.
Löschen von Daten auf nicht flüchtigen elektronischen Speichermedien (Solid State Disks)	Verwendung von Löschbefehlen (z.B. ATA Secure Erase) oder vorherige Verschlüsselung und Löschung des Schlüssels.	Teilweise Unwiderruflichkeit der Vernichtung gegeben.